eSecurity

# Treinamentos em Segurança da Informação

# O que temos para hoje?



Menu do dia:

- ✓ **Brute Force:**
  - ✓ Rainbow Tables
  - ✓ Reduce Function
  - ✓ Criando sua Rainbow Tables
  - ✓ Indexando sua RT
  - ✓ Quebrando Hashes com Rainbow Crack
  - ✓ Quebrando Hashes com Ophcrack

# Brute Force

# Brute Force: Reduce Function



**Reduce Function**
Para entender as funções de redução, vamos olhar para um conjunto de valores de dois dígitos que são "criptografadas" em hashes de quatro dígitos.
Por exemplo, usando o algoritmo de hash, o número 10 é criptografada em 0823.

**Vamos lá**:
Passowrd (P) = 10
Hash (H) = 0823

Agora, imagine se tivéssemos uma função especial que pudesse de alguma forma mapear um hash de 4 dígitos para um número de 2 dígitos. Porque hashes são irreversíveis então o número de dois dígitos não é a senha original. Mas, é um número de dois dígitos, o que significa que é uma senha válida. Por exemplo, uma função de redução realmente simples pode levar os dois últimos dígitos de um número de quatro dígitos. Isso seria mapear o hash em 0823 o texto plano 23.

# Brute Force: Reduce Function



**Reduce Function**
Isso é tudo uma função de redução é - uma função que mapeia de forma consistente um valor de hash em um valor de texto simples válido. Vale a pena repetir que a função do órgão redução não é o inverso do hash. No exemplo acima, 0823 "reduz" a 23, 23 mas não de hash em 0823 (23 hash em 5603)

| p1 | h1=H(p1) | p2=R1(h1) | h2=H(p2) | p3=R2(h2) | h3=H(p3) |
|---|---|---|---|---|---|
| 3 | 3955 | 55 | 4532 | 45 | 3708 |
| 10 | 0823 | 23 | 5603 | 56 | 5850 |
| 25 | 2059 | 59 | 3626 | 36 | 4202 |
| 68 | 3131 | 31 | 3790 | 37 | 5520 |
| 91 | 2554 | 54 | 3213 | 32 | 5109 |

| p1 | h3 |
|---|---|
| 3 | 3708 |
| 10 | 5850 |
| 25 | 4202 |
| 68 | 5520 |
| 89 | 5109 |

# Brute Force: Criando Rainbow Tables



**The Rainbow Crack**
O RainbowCrack é um conjunto de ferramentas para desenvolvimento e quebra hashes por consulta à Rainbow Tables.

**Seus principais aplicativos são:**

**rtgen:** Para criar a Rainbow Tables

**rtsort:** Para organizar as Chains criadas e disponibiliza-las em ordem para uma rápida pesquisa

**rcrack:** Para realizar a quebra da hash

# Brute Force: Criando Rainbow Tables



**Sintaxe:**
*rtgen hash_algorithm charset plaintext_len_min plaintext_len_max table_index chain_len chain_num part_index*

**Explicação:**
**hash_algorithm:** O algoritmo dos hashs (lm, ntlm, md5 e assim por diante) usado na rainbow table.
**charset:** A configuração dos caracteres (charset) do texto plano na rainbow tables. Todos os charsets possíveis estão definidos no arquivo charset.txt.
**plaintext_len_min e plaintext_len_max:** Estes dois parâmetros definem o tamanho possível de todo o texto plano na 'rainbow tables'. Se o 'charset' é numérico, o 'plaintext_len_min' é 1, e o 'plaintext_len_max' é 5, então a string "12345" será incluída na tabela, mas "123456" não.

# Brute Force: Rainbow Tables



**table_index, chain_len, chain_num e part_index:** Estes quatro parâmetros são:

- O 'table_index' está relacionado ao 'reduce function' que é utilizado na 'rainbow table'.
- O 'chain_len' é o tamanho de cada 'rainbow chain' na 'rainbow table'. Uma 'rainbow chain' configurada como 16 bytes é a menor unidade em uma 'rainbow table'. Uma 'rainbow tables' contém diversas 'rainbow chains'.
- O 'chains_num' é o número de 'rainbow chains' em uma 'rainbow table'.
- O parâmetro 'part_index' determina como o 'start point' em cada 'rainbow chain' é gerado. Deve ser um número (ou começar com um número).

**Exemplo:**

*rtgen md5 loweralpha-numeric 1 7 0*

*rtgen md5 loweralpha-numeric 1 7 0  -bench*

# Brute Force: Rainbow Tables



Após esse processo devemos então organizar nossa lista e deixa-la indexada para agilizar o processo da quebra.

**Para isso utilizamos a ferramenta rtsort:**
*rtsort *.rt*

**Depois desse processo, basta realizar a tentativa da quebra com o commando rcrack:**

*rcrack *.rt -h 5d41402abc4b2a76b9719d911017c592*
*rcrack *.rt -l hash.txt*

# Brute Force: Quebrando Hash



Agora que já temos a noção de como rainbow tables trabalha, vamos então colocar em prática e quebrar alguma hash do Windows.

Obtivemos a conta de um administratdor e sua senha mullet para tentar realizar a quebra do modo mais rápido possível.

1. Primeiro temos que baixar a tabela de hashes do Windows XP/2003

2. Depois precisamos realizar a importação dessas hashes no Ophcrack

3. Inserir a hash ou a SAM a ser quebrada

4. Realizar o crack

# Chega por hoje



www.eSecurity.com.br

**E-mail**: alan.sanches@esecurity.com.br

**Twitter**: @esecuritybr e @desafiohacker

**Skype**: desafiohacker

**Fanpage**: www.facebook.com/academiahacker